I

Compléments sur les groupes

I.1 Sous-groupe engendré par une partie

1. ➙ **Intersection de sous-groupes**
Soit $(H_k)_{k\in I}$, une famille de sous-groupes de $(G,*)$. Leur intersection

$$H=\bigcap_{k\in I} H_k$$

est un sous-groupe de $(G,*)$.

2. **Parties génératrices d'un groupe**
On considère un groupe $(G,\star)$ et une partie S de G.
2.1 L'intersection G_1 des sous-groupes H de G contenant S est un sous-groupe de G qui contient S.
Tout sous-groupe de G qui contient S contient aussi G_1.
2.2 L'ensemble G_2 des $x\in G$ tels que

$$\exists\, n\in\mathbb{N}^*,\ \exists\,(s_1,\dots,s_n)\in S^n,\exists\,(\alpha_1,\dots,\alpha_n)\in\mathbb{Z}^n,\quad x=s_1^{\alpha_1}\star\cdots\star s_n^{\alpha_n}.$$

est un sous-groupe de G qui contient S.
Tout sous-groupe de G qui contient S contient aussi G_2.
2.3 ✍ *Soient $(G,\star)$, un groupe et S, une partie de G. Le* **sous-groupe engendré par** *S, noté $\langle S\rangle$, est le plus petit sous-groupe H de G tel que $S\subset H$.*

3. **Exemples**
3.1 Si a_1, …, a_p commutent deux à deux, un élément x de G appartient au sous-groupe engendré par a_1, …, a_p si, et seulement si,

$$\exists\,(\alpha_1,\dots,\alpha_p)\in\mathbb{Z}^p,\quad x=a_1^{\alpha_1}\star\cdots\star a_p^{\alpha_p}$$

ou, dans le cas où $\star=+$,

$$\exists\,(\alpha_1,\dots,\alpha_p)\in\mathbb{Z}^p,\quad x=\sum_{k=1}^{p}\alpha_k\,a_k.$$

3.2 Le groupe $(\mathbb{Z},+)$ est engendré par 1.
3.3 Le groupe $(\mathbb{U}_n,\times)$ des racines n-ièmes de l'unité est engendré par $\exp(2i\pi/n)$.
3.4 Le groupe symétrique $(\mathfrak{S}_n,\circ)$ est engendré par les transpositions $\tau_{i,j}$, $1\leqslant i<j\leqslant n$.
Il est aussi engendré par les transpositions $\tau_{1,i}$, $1\leqslant i\leqslant n$, ainsi que par la transposition $\tau_{1,2}$ et le cycle $(1\quad 2\quad 3\quad\cdots\quad n)$.
Il est enfin engendré par la famille des cycles.
3.5 Le groupe $\big(\mathrm{GL}_n(\mathbb{R}),\times\big)$ est engendré par les matrices de transvection et les matrices de dilatation.

I.2 Groupes monogènes

4. ➙ *Dans un groupe multiplicatif, le sous-groupe $\langle a\rangle$ engendré par un élément $a\in G$ peut être décrit en extension :*

$$\langle a\rangle=\{a^k,\ k\in\mathbb{Z}\}.$$

Dans un groupe additif,

$$\langle a\rangle=\{k\cdot a,\ k\in\mathbb{Z}\}.$$

5.1 ✍ *Un groupe $(G,\star)$ est* **monogène** *lorsqu'il est engendré par un élément de G :*

$$\exists\, a\in G,\quad \langle a\rangle=G.$$

5.2 Un groupe monogène est commutatif.
5.3 Le groupe $(\mathbb{Z},+)$ est monogène.
5.4 Pour tout entier $n\in\mathbb{N}$, l'ensemble $n\mathbb{Z}$ est un sous-groupe monogène de $(\mathbb{Z},+)$.
5.5 Si G est un sous-groupe de $(\mathbb{Z},+)$ qui n'est pas réduit à $\{0\}$, alors l'ensemble $G_0=G\cap\mathbb{N}^*$ possède un plus petit élément.
5.6 ➙ **Sous-groupes additifs de $\mathbb{Z}$**
Tout sous-groupe H de $(\mathbb{Z},+)$ est monogène et il existe un, et un seul, entier $n\in\mathbb{N}$ tel que $H=n\mathbb{Z}$.

6.1 ✍ *Un groupe $(G,\star)$ est* **cyclique** *lorsqu'il est monogène et fini.*
6.2 ✍ *L'***ordre d'un groupe** *$(G,\star)$ est le cardinal de l'ensemble G.*
6.3 Le groupe $(\mathbb{U}_n,\times)$ est cyclique.

Morphismes

7. ➙ *Soient $(G,\star)$, un groupe monogène ; $g\in G$, un générateur de G et $(H,\otimes)$, un groupe.*
Pour tout $h\in H$, il existe au plus un morphisme de groupes f de $(G,\star)$ dans $(H,\otimes)$ tel que $f(g)=h$.

8. Pour tout élément a de G, on considère l'application φ_a de $\mathbb{Z}$ dans G définie par

$$\varphi_a=[k\mapsto a^k]$$

ou par $\varphi_a=[k\mapsto k\cdot a]$ si l'opération sur G est une addition.
8.1 L'application φ_a est un morphisme de groupes de $(\mathbb{Z},+)$ dans $(G,\star)$.
8.2 L'image de φ_a est le sous-groupe $\langle a\rangle$.
8.3 Si φ_a est injectif, alors l'ordre du groupe $\langle a\rangle$ est infini.
8.4 Si φ_a n'est pas injectif, alors il existe un, et un seul, entier $n\geqslant 1$ tel que le noyau de φ_a soit égal à $n\mathbb{Z}$. Le sous-groupe $\langle a\rangle$ est alors un groupe cyclique d'ordre n :

$$\langle a\rangle=\{e_G,a,\dots,a^{n-1}\}$$

et $a^n=e_G$.

9. Soit $\langle a\rangle$, un groupe cyclique d'ordre $n\in\mathbb{N}^*$.
9.1 Pour tout morphisme de groupes $f:\langle a\rangle\to H$, l'ordre de $f(a)$ est un diviseur de n.
9.2 Soit $\langle y_0\rangle$, un sous-groupe cyclique d'ordre q de H tel que q divise n.

1. Si $a^{k_1}=a^{k_2}$, alors $y_0^{k_1}=y_0^{k_2}$.
2. L'application $f=[a^k\mapsto y_0^k]$ est l'unique morphisme de groupes de $\langle a\rangle$ dans H tel que $f(a)=y_0$. →**[22]**

L'image de ce morphisme est le sous-groupe $\langle y_0\rangle$.
Si l'ordre de y_0 est égal à n, alors ce morphisme est injectif.

10. ➙ *Soient $\langle a\rangle$, un groupe cyclique d'ordre $n\in\mathbb{N}^*$ et y_0, un élément du groupe $(H,\otimes)$.*
10.1 *Il existe un morphisme de groupes $f:\langle a\rangle\to H$ tel que $f(a)=y_0$ si, et seulement si, le sous-groupe $\langle y_0\rangle$ est un groupe cyclique dont l'ordre divise n.*
10.2 *Ce morphisme induit un isomorphisme de $\langle a\rangle$ sur $\langle y_0\rangle$ si, et seulement si, l'ordre de $\langle y_0\rangle$ est égal à n.*

11. ➙ **Classification des groupes monogènes**
Un groupe monogène infini est isomorphe à $(\mathbb{Z},+)$.
Un groupe cyclique d'ordre $n\in\mathbb{N}$ est isomorphe à $(\mathbb{U}_n,\times)$. →**[22.7]**

12. **Exemples**

1. Le seul morphisme de groupes de $\mathbb{U}_5$ dans $\mathbb{U}_6$ est le morphisme trivial : $[x\mapsto 1]$.
2. Si f est un automorphisme de $\mathbb{U}_4$, alors $f(i)$ est un élément d'ordre 4. Les automorphismes de $\mathbb{U}_4$ sont $[x\mapsto x]$ et $[x\mapsto\overline{x}]$.
3. Il existe autant de morphismes de groupes de $\mathbb{U}_n$ dans $\mathbb{U}_m$ que d'éléments de $\mathbb{U}_m$ dont l'ordre divise n.

I.3 Ordre d'un élément

13.1 ✍ *L'***ordre d'un élément** $a \in G$ *est l'ordre du sous-groupe* $\langle a \rangle$.
13.2 ➙ *Si* $a \in G$ *est un élément d'ordre* d, *alors*

$$\langle a \rangle = \{e_G,\, a,\, a^2, \ldots, a^{d-1}\}.$$

Si G *est un groupe additif,*

$$\langle a \rangle = \{0_G,\, a,\, 2 \cdot a, \ldots, (d-1) \cdot a\}.$$

13.3 ➙ *Si l'ordre d'un élément* $a \in G$ *est égal à* d, *alors*

$$a^n = e_G \iff d \mid n.$$

Dans un groupe additif,

$$n \cdot a = 0_G \iff d \mid n.$$

13.4 Un groupe G d'ordre n est cyclique si, et seulement si, il existe un élément $a \in G$ d'ordre n.

14. Théorème de Lagrange
14.1 Soit $(G, \star)$, un groupe commutatif d'ordre $n \in \mathbb{N}^*$.
Pour tout $a \in G$, l'application $[x \mapsto a \star x]$ est une bijection de G sur G, donc

$$\prod_{x \in G} x = \prod_{x \in G} (a \star x)$$

et $a^n = e_G$.
14.2 ➙ *Si* $(G, \star)$ *est un groupe fini, alors l'ordre de tout élément* a *de* G *divise l'ordre de* G.
14.3 Le théorème **[14.2]** est vrai également pour les groupes non commutatifs. →**[74]**

Entraînement

15. Questions pour réfléchir
1. Le groupe $(\mathbb{U}, \times)$ est-il monogène ?
2. Pour $n \geqslant 3$, le groupe symétrique $(\mathfrak{S}_n, \circ)$ n'est pas cyclique.
3. Si $(G, \star)$ est un groupe commutatif, alors l'application

$$[x \mapsto x^n] : G \to G$$

est un morphisme de groupe pour tout entier $n \in \mathbb{Z}$.

16. L'ensemble $G = \{\pm 1\} \times \{\pm 1\}$ muni de la loi de composition définie par

$$(g_1, g_2) \star (h_1, h_2) = (g_1 g_2,\, h_1 h_2)$$

est un groupe commutatif d'ordre 4. Ce groupe est engendré par les éléments $(1, -1)$ et $(-1, 1)$, mais il n'est pas cyclique.

17. Sous-groupes d'un groupe monogène [11]
17.1 L'image réciproque d'un sous-groupe H de $(G, \star)$ par le morphisme $\varphi_a : \mathbb{Z} \to G$ est un sous-groupe de $(\mathbb{Z}, +)$.
17.2 Un sous-groupe d'un groupe monogène est monogène.

18. Racines primitives de l'unité
Une racine n-ième de l'unité est une ***racine primitive*** lorsqu'elle engendre le groupe $\mathbb{U}_n$.
1. La racine n-ième de l'unité $\zeta_k = \exp(2ik\pi/n)$ est une racine primitive si, et seulement si, l'entier k est premier à n.
2. Décrire, en fonction de k, le sous-groupe de $\mathbb{U}_n$ engendré par ζ_k.

19. On suppose qu'un groupe fini G contient un élément x d'ordre 3 et un élément y d'ordre 5.
1. L'ordre de G est divisible par 15.
2. Si $x \star y = y \star x$, alors G contient un élément d'ordre 15.

20. Sous-groupes additifs de $\mathbb{R}$
Contrairement à $(\mathbb{Z}, +)$, le groupe $(\mathbb{R}, +)$ contient des sous-groupes qui ne sont pas monogènes.
20.1 Soit G, un sous-groupe monogène de $(\mathbb{R}, +)$, qui n'est pas réduit au singleton $\{0\}$. Il existe un plus petit élément $g > 0$ dans G et $G = \langle g \rangle = g\mathbb{Z}$.
20.2 Soient a et b, deux réels strictement positifs. Si le sous-groupe

$$\langle a, b \rangle = \langle a \rangle + \langle b \rangle$$

est monogène, alors le quotient a/b est rationnel.
20.3 Un sous-groupe G de $(\mathbb{R}, +)$ qui n'est pas monogène est dense dans $\mathbb{R}$.

21. Soient H_1 et H_2, deux sous-groupes de $(G, +)$.
21.1 La somme

$$H_1 + H_2 = \{x + y\,, (x, y) \in H_1 \times H_2\}$$

est un sous-groupe de G qui contient H_1 et H_2.
21.2 En revanche, l'union $H_1 \cup H_2$ est un sous-groupe de G si, et seulement si,

$$H_1 \subset H_2 \qquad \text{ou} \qquad H_2 \subset H_1.$$

22. Quotient d'un groupe commutatif
Soient $(G, \star)$, un groupe commutatif ; $(H, \bullet)$, un groupe et f, un morphisme de groupes de G dans H.
22.1 ✍ *Pour tout* $x \in G$, *la* **classe de** x **modulo** $\operatorname{Ker} f$ *est définie par*

$$\mathscr{C}(x) = \{x \star h,\, h \in \operatorname{Ker} f\}.$$

L'ensemble des classes modulo $\operatorname{Ker} f$

$$G/\operatorname{Ker} f = \{\mathscr{C}(x),\, x \in G\}$$

est appelé le **quotient de** G **par** $\operatorname{Ker} f$.
22.2 La relation binaire $\sim$ définie par

$$\forall\, x, y \in G, \qquad x \sim y \iff \mathscr{C}(x) = \mathscr{C}(y)$$

est une relation d'équivalence sur G et les classes modulo $\operatorname{Ker} f$ sont les classes d'équivalence de cette relation d'équivalence.
22.3 ✍ *Quels que soient* x *et* y *dans* G, *on pose*

$$\mathscr{C}(x) \otimes \mathscr{C}(y) = \mathscr{C}(x \star y).$$

22.4 Si $\mathscr{C}(x_1) = \mathscr{C}(x_2)$ et $\mathscr{C}(y_1) = \mathscr{C}(y_2)$, alors

$$\mathscr{C}(x_1 \star y_1) = \mathscr{C}(x_2 \star y_2).$$

Par conséquent, l'opération $\otimes$ est une loi de composition interne, associative et commutative sur le quotient $G/\operatorname{Ker} f$.
22.5 L'opération $\otimes$ définit une structure de groupe sur $G/\operatorname{Ker} f$, dont l'élément neutre est $\mathscr{C}(e_G)$.
L'application $\mathscr{C}$ est alors un morphisme de groupes de G sur $G/\operatorname{Ker} f$. Ce morphisme de groupes est surjectif ; son noyau est égal à $\operatorname{Ker} f$.
22.6 Pour tout élément $C \in G/\operatorname{Ker} f$, il existe $x \in G$ tel que $C = \mathscr{C}(x)$ et on pose alors

$$\varphi(C) = f(x).$$

1. L'application $\varphi : G/\operatorname{Ker} f \to H$ est bien définie.
2. L'application φ est un morphisme de groupes injectif.
3. Si le morphisme f est surjectif, alors φ réalise un isomorphisme de $G/\operatorname{Ker} f$ sur H.

22.7 Soient $n \geqslant 2$, un entier et $\zeta = \exp(2i\pi/n)$. L'application

$$f = \left[k \mapsto \zeta^k\right]$$

est un morphisme de groupes de $(\mathbb{Z}, +)$ dans $(\mathbb{U}_n, \cdot)$ qui induit un isomorphisme du groupe additif $(\mathbb{Z}/n\mathbb{Z}, \oplus)$ sur le groupe multiplicatif $(\mathbb{U}_n, \cdot)$. →**[11]**

II

Anneaux et corps

23. Exemples et contre-exemples
On identifie un anneau $(A,+,\star)$ à l'ensemble A lorsque les opérations sont usuelles.

23.1 Anneaux de nombres

1. Les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des anneaux. L'ensemble des ***entiers de Gauss*** :

$$\mathbb{Z}[i] = \{a+ib,\ (a,b)\in\mathbb{Z}^2\}$$

est un sous-anneau de $\mathbb{C}$.

2. L'ensemble $\mathbb{N}$ n'est pas un anneau.

23.2 Anneau des polynômes

3. L'ensemble $\mathbb{R}[X]$ des polynômes à coefficients réels et l'ensemble $\mathbb{R}(X)$ des fractions rationnelles à coefficients réels sont des anneaux.

4. Quel que soit l'entier $n\geqslant 1$, l'ensemble $\mathbb{R}_n[X]$ des polynômes dont le degré est inférieur à n n'est pas un anneau.

23.3 Anneaux de matrices

5. L'ensemble $\mathfrak{M}_n(\mathbb{C})$ des matrices carrées à coefficients complexes est un anneau (non commutatif).
Les ensembles $U_n(\mathbb{C})$ et $L_n(\mathbb{C})$ des matrices carrées triangulaires supérieures et triangulaires inférieures sont des anneaux (non commutatifs).
L'ensemble $D_n(\mathbb{C})$ des matrices carrées diagonales est un anneau commutatif.

6. L'ensemble $\mathrm{GL}_n(\mathbb{C})$ des matrices inversibles n'est pas un anneau, pas plus que l'ensemble $O_n(\mathbb{R})$ des matrices orthogonales.

23.4 Anneau des endomorphismes
L'ensemble $\mathrm{L}(E)$ des endomorphismes de E est un anneau. La loi multiplicative est $\circ$, l'élément unité est I_E.

23.5 Anneau booléen
Pour tout ensemble E, le triplet $(\mathfrak{P}(E),\Delta,\cap)$ est un anneau commutatif.

23.6 Familles sommables
L'ensemble $\ell^1(\mathbb{N})$ des familles complexes sommables indexées par $\mathbb{N}$ est un anneau pour l'addition des suites et le produit de Cauchy.

Éléments remarquables d'un anneau

24. Éléments inversibles

24.1 ✍ *Soit $(A,+,\star)$, un anneau. Un élément x de A est* **inversible** *lorsqu'il existe $y\in A$ tel que*

$$x\star y = y\star x = 1_A.$$

24.2 Si x est inversible dans l'anneau $(A,+,\star)$, alors il existe un, et un seul, élément y de A tel que $x\star y = y\star x = 1_A$.

24.3 Si x et y sont deux éléments inversibles de $(A,+,\star)$, alors $x\star y$ est inversible et

$$(x\star y)^{-1} = y^{-1}\star x^{-1}.$$

24.4 ➙ *L'ensemble $A^\star$ des éléments inversibles de l'anneau $(A,+,\star)$ est un groupe pour la loi $\star$.*

25. Éléments nilpotents
Soit $(A,+,\star)$, un anneau.

25.1 ✍ *Un élément x de A est dit* **nilpotent** *lorsqu'il existe $n\in\mathbb{N}$ tel que $x^n = 0_A$.*

25.2 Un élément nilpotent n'est pas inversible.

25.3 ✍ *L'***indice de nilpotence** *de x est le plus petit élément de*

$$\{n\in\mathbb{N}\ :\ x^n = 0_A\}.$$

25.4 Si x est nilpotent, alors l'indice de nilpotence de x est le seul entier $n\in\mathbb{N}^*$ tel que $x^n = 0_A$ et $x^{n-1}\neq 0_A$.

25.5 Si $x^n = 0_A$, alors $(1_A - x)$ est inversible et

$$(1_A - x)^{-1} = \sum_{k=0}^{n-1} x^k.$$

26. Diviseurs de zéro

26.1 ✍ *Soit $(A,+,\star)$, un anneau. Un élément x non nul de A est un* **diviseur de zéro à gauche** *(resp.* **à droite***) lorsqu'il existe un élément y non nul de A tel que $x\star y = 0_A$ (resp. $y\star x = 0_A$).*

26.2 Un diviseur de zéro n'est pas inversible.

26.3 Tout élément nilpotent non nul est un diviseur de zéro.

26.4 ✍ *Un* **anneau intègre** *est un anneau commutatif sans diviseur de zéro.*

Morphismes d'anneaux

27. Un morphisme d'anneaux est une application d'un ensemble A dans un ensemble B, compatible avec les structures d'anneaux définies sur A et B.

28. ✍ *Soient $(A,+,\star)$ et $(B,\oplus,\otimes)$, deux anneaux. Une application $\varphi : A\to B$ est un* **morphisme d'anneaux** *lorsque*

$$\forall\,(x,y)\in A\star A,\quad \varphi(x+y) = \varphi(x)\oplus\varphi(y) \tag{1}$$

$$\forall\,(x,y)\in A\star A,\quad \varphi(x\star y) = \varphi(x)\otimes\varphi(y) \tag{2}$$

$$\varphi(1_A) = 1_B. \tag{3}$$

29. Soit $\varphi : A\to B$, un morphisme d'anneaux.

29.1 Pour tout $x\in A$ et tout $n\in\mathbb{Z}$,

$$\varphi(n\cdot x) = n\cdot\varphi(x)$$

et en particulier, $\varphi(0_A) = 0_B$.

29.2

$$\forall\, x\in A,\ \forall\, n\in\mathbb{N},\quad \varphi(x^{\star n}) = \big[\varphi(x)\big]^{\otimes n}$$

29.3 ➙ *Si x est un élément inversible de A, alors $\varphi(x)$ est un élément inversible de B et*

$$\big[\varphi(x)\big]^{-1} = \varphi(x^{-1}).$$

29.4 Si $x\in A$ est nilpotent, alors $\varphi(x)$ est nilpotent et son indice de nilpotence est inférieur à celui de x.

30. ✍ *Soit $\varphi : (A,+,\star)\to(B,\oplus,\otimes)$, un morphisme d'anneaux. Le* **noyau** *de φ est défini par*

$$\operatorname{Ker}\varphi = \big\{x\in A\ :\ \varphi(x) = 0_B\big\}.$$

31. ✍ *Un* **isomorphisme d'anneaux** *de $(A,+,\star)$ sur $(B,\oplus,\otimes)$ est une application bijective $\varphi : A\to B$ qui est un morphisme d'anneaux de $(A,+,\star)$ dans $(B,\oplus,\otimes)$.*

32. Soit $\varphi : A\to B$, un isomorphisme d'anneaux.

32.1 La bijection réciproque φ^{-1} est un morphisme d'anneaux de $(B,\oplus,\otimes)$ dans $(A,+,\star)$.

32.2 ➙ *Un élément $x\in A$ est inversible si, et seulement si, son image $\varphi(x)\in B$ est inversible.*

32.3 Si $x\in A$ est nilpotent d'indice n, alors $\varphi(x)$ est aussi nilpotent d'indice n.

32.4 Si $x\in A$ est un diviseur de zéro, alors $\varphi(x)$ est aussi un diviseur de zéro.

II.1 Produit fini d'anneaux

33. Soient $(A_1,+,\star)$ et $(A_2,+,\otimes)$, deux anneaux. Sur le produit

$$A = A_1\times A_2$$

on définit les opérations $\oplus$ et $\bullet$ par

$$(x_1,x_2)\oplus(y_1,y_2) = (x_1+y_1,\,x_2+y_2)$$
$$(x_1,x_2)\bullet(y_1,y_2) = (x_1\star y_1,\ x_2\otimes y_2).$$

33.1 L'ensemble $A_1\times A_2$ muni des opérations $\oplus$ et $\bullet$ est un anneau.

33.2 ✍ *L'anneau $(A_1 \times A_2, \oplus, \bullet)$ est l'***anneau produit** *de l'anneau $(A_1, +, \star)$ par l'anneau $(A_2, +, \otimes)$.*
33.3 L'élément nul de l'anneau produit est $(0_{A_1}, 0_{A_2})$; l'élément unité est $(1_{A_1}, 1_{A_2})$.
33.4 L'élément (x_1, x_2) est inversible si, et seulement si, x_1 et x_2 sont inversibles. Dans ce cas,

$$(x_1, x_2)^{-1} = (x_1^{-1}, x_2^{-1}).$$

33.5 L'anneau produit $(A_1 \times A_2, \oplus, \bullet)$ est commutatif si, et seulement si, les deux anneaux $(A_1, +, \star)$ et $(A_2, +, \otimes)$ sont commutatifs.
33.6 L'anneau produit $(A_1 \times A_2, \oplus, \bullet)$ n'est pas intègre :

$$(0,1) \bullet (1,0) = (0,0)$$

même si les anneaux A_1 et A_2 sont intègres.

34. Morphismes
34.1 ✍ *Les* **projections canoniques** *sont les applications définies par*

$$\pi_1 : \begin{array}{ccc} A_1 \times A_2 & \to & A_1 \\ (x_1, x_2) & \mapsto & x_1 \end{array} \quad \textit{et} \quad \pi_2 : \begin{array}{ccc} A_1 \times A_2 & \to & A_2 \\ (x_1, x_2) & \mapsto & x_2 \end{array}.$$

34.2 Les projections canoniques sont des morphismes d'anneaux surjectifs.
34.3 ➸ *Une application*

$$\begin{array}{rcl} \theta : L & \to & A_1 \times A_2 \\ x & \mapsto & \big(\varphi(x), \psi(x)\big) \end{array}$$

est un morphisme d'anneaux de $(L, +, \top)$ dans $(A_1 \times A_2, +, \bullet)$ si, et seulement si, les applications $\varphi : L \to A_1$ et $\psi : L \to A_2$ sont des morphismes d'anneaux.
34.4 Les injections définies par

$$i_1 : \begin{array}{ccc} A_1 & \to & A_1 \times A_2 \\ x_1 & \mapsto & (x_1, 0_{A_2}) \end{array} \quad \text{et} \quad i_2 : \begin{array}{ccc} A_2 & \to & A_1 \times A_2 \\ x_2 & \mapsto & (0_{A_1}, x_2) \end{array}$$

ne sont pas des morphismes d'anneaux.

II.2 Idéaux d'un anneau commutatif

35. ✍ *Soit $(A, +, \star)$, un anneau* commutatif. *Une partie I de A est un* **idéal** *de A lorsque*
1. *I est un sous-groupe de $(A, +)$*
2. *qui est* **absorbant** *pour $\star$:*

$$\forall\, x \in I,\ \forall\, y \in A, \quad x \star y \in I.$$

36. ➸ *Le noyau d'un morphisme d'anneaux $\varphi : A \to B$ est un idéal de A.*
37.1 Les idéaux d'un corps commutatif $\mathbb{K}$ sont $\{0\}$ et $\mathbb{K}$.
37.2 Un morphisme d'anneaux d'un corps commutatif $\mathbb{K}$ dans un corps commutatif $\mathbb{L}$ est injectif.
L'existence d'un tel morphisme permet de voir $\mathbb{K}$ comme un sous-corps de $\mathbb{L}$.

38. Idéal engendré par un élément
38.1 Pour tout $x \in A$, l'ensemble

$$xA = \{x \star y,\ y \in A\}$$

est un idéal de A.
38.2 ✍ *Pour tout $x \in A$, l'idéal xA, aussi noté $\langle x \rangle$, est appelé* **idéal engendré par** *x.*
38.3 Soit I, un idéal de A. Alors :

$$x \in I \iff xA \subset I$$

et en particulier

$$I = A \iff 1_A \in I.$$

39. Opération sur les idéaux
39.1 Si I et J sont deux idéaux de A, alors $I \cap J$ est un idéal de A et tout idéal H contenu dans I et dans J est aussi contenu dans $I \cap J$.
39.2 Si I et J sont deux idéaux de A, alors $I + J$ est un idéal de A et tout idéal H qui contient I et J contient aussi $I + J$.
39.3 ➸ *L'idéal $xA + yA$ est le plus petit idéal de A contenant à la fois x et y.*

II.3 Divisibilité dans un anneau intègre

40. Anneaux intègres [26.4]
40.1 Un corps est un anneau intègre.
Les anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$, qui ne sont pas des corps, sont intègres.
Les anneaux $\mathfrak{M}_3(\mathbb{R})$ et $\mathbb{Z}/6\mathbb{Z}$ ne sont pas intègres.
40.2 ➸ **Simplification dans un anneau intègre**
Soit A, un anneau intègre et $z \neq 0_A$. Si $x \star z = y \star z$, alors $x = y$.

41.1 ✍ *Dans un anneau intègre $(A, +, \star)$, on dit que $x \in A$* **divise** *$y \in A$ (ou que y est un* **multiple** *de x) lorsque*

$$\exists\, q \in A, \quad y = q \star x.$$

On note alors $x \mid y$.
41.2 ➸

$$x \mid y \iff yA \subset xA$$

42. Éléments inversibles
42.1 Un élément x de A est inversible si, et seulement si, il divise 1_A.
42.2 ➸ *Un élément x de A est inversible si, et seulement si, l'idéal xA est égal à A.*

$$x \in A^\star \iff xA = A$$

42.3 S'il existe $n \in \mathbb{N}^*$ tel que x^n soit inversible, alors x est inversible.
42.4 Exemples fondamentaux
1. Les éléments inversibles de $\mathbb{Z}$ sont 1 et -1.
2. Les éléments inversibles de $\mathbb{K}[X]$ sont les polynômes constants non nuls, c'est-à-dire les polynômes dont le degré est nul.

43. Éléments associés
43.1 ✍ *Deux éléments x et y d'un anneau intègre A sont* **associés** *lorsqu'ils engendrent le même idéal : $xA = yA$.*
43.2 ➸ *Deux éléments x et y de A sont associés si, et seulement si, il existe un élément inversible $u \in A^\times$ tel que $y = u \star x$.*
43.3 ▷ *Les éléments inversibles de A sont les éléments associés à 1_A.*

44. Éléments irréductibles
Soit A, un anneau intègre.
44.1 ✍ *Un élément non nul de A qui peut s'écrire comme le produit de deux éléments non inversibles de A est dit* **composé**.
44.2 Un entier $x \in \mathbb{N}$ est composé si, et seulement si, il existe deux entiers $y \geqslant 2$ et $z \geqslant 2$ tels que $x = yz$.
44.3 Un polynôme $P \in \mathbb{K}[X]$ est composé si, et seulement si, il existe deux polynômes Q_1 et Q_2 tels que $P = Q_1 Q_2$ avec $\deg Q_1 \geqslant 1$ et $\deg Q_2 \geqslant 1$.
44.4 Si x est le produit de deux éléments y et z non inversibles, alors

$$xA \subsetneq yA \subsetneq A \quad \text{et} \quad xA \subsetneq zA \subsetneq A.$$

44.5 ✍ *Un élément non nul de A est* **irréductible** *lorsqu'il n'est ni inversible, ni composé.*
44.6 Si un élément irréductible x est factorisé sous la forme $x = y \star z$ avec z non inversible, alors y est inversible. Autrement dit :

$$(xA \subsetneq yA) \implies (yA = A).$$

Anneaux euclidiens

45. Les seuls anneaux intègres intéressants que nous rencontrerons sont l'anneau $\mathbb{Z}$ des entiers relatifs et l'anneau $\mathbb{K}[X]$ des polynômes sur un corps $\mathbb{K} \subset \mathbb{C}$. Il se trouve que ces deux anneaux sont munis d'une division euclidienne, ce qui simplifie considérablement la structure de leurs idéaux : tous les idéaux sont engendrés par un élément. →**[38]**

46. ➸ **Idéaux de $\mathbb{Z}$ [5.6]**
Pour tout idéal I de $\mathbb{Z}$, il existe un, et un seul, entier $n \in \mathbb{N}$ tel que

$$I = n\mathbb{Z}.$$

47. Idéaux de $\mathbb{K}[X]$
Soit I, un idéal de $\mathbb{K}[X]$, non réduit à $\{0\}$.
47.1 Si P et Q sont deux polynômes appartenant à I, alors le reste de la division euclidienne de P par Q appartient à I.
47.2 L'idéal I est engendré par tout polynôme $P_0 \in I$ tel que

$$\deg P_0 = \min\{\deg P,\ P \in I \setminus \{0\}\}.$$

47.3 ⇝ *Pour tout idéal $I \subset \mathbb{K}[X]$ non réduit à $\{0\}$, il existe un, et un seul, polynôme unitaire $P_0 \in \mathbb{K}[X]$ tel que I soit engendré par P_0.*

Entraînement

48. Questions pour réfléchir
1. Soient x et y, deux éléments d'un anneau A.
1.a Si $xy = 1_A$, l'élément x est-il inversible ?
1.b Si x est inversible et si $xy = 1_A$, alors $yx = 1_A$.
2. Soit B, un sous-anneau de A. Un élément $x \in B$ peut être inversible en tant qu'élément de A sans être inversible en tant qu'élément de B.
3. L'indice de nilpotence peut-il être nul ? égal à 1 ?
4. L'indice de nilpotence de x est inférieur à n si, et seulement si, $x^n = 0$.
5. Un produit d'éléments nilpotents est-il encore un élément nilpotent ?
6. *Suite de* **[29]** –
6.a Est-il possible que $\varphi(x)$ soit inversible sans que x soit inversible ?
6.b Si x est un diviseur de zéro, $\varphi(x)$ est-il encore un diviseur de zéro ?
7. Quels sont les éléments nilpotents d'un anneau produit ?
8. On suppose que les seuls idéaux de l'anneau commutatif A sont $\{0\}$ et A.
8.a Si $x \neq 0$, alors l'élément unité 1_A appartient à l'idéal xA engendré par x.
8.b L'anneau A est en fait un corps.
9. *Suite de* **[41.1]** – Si un élément x non nul divise y, alors il existe un, et un seul, élément $q \in A$ tel que $y = q \star x$.
10. Pourquoi la notion de divisibilité est-elle sans intérêt dans un corps ?

49. Factorisation d'un morphisme d'anneaux [22]
Soient $(A, +, \star)$ et $(B, +, \bullet)$, deux anneaux commutatifs et f, un morphisme d'anneaux de A dans B. On définit les classes modulo $I = \operatorname{Ker} f$ par

$$\forall\, x \in A, \quad \mathscr{C}(x) = \{x + h,\ h \in \operatorname{Ker} f\}$$

et on note A/I, l'ensemble des classes.
49.1 Les classes modulo I forment une partition de A et

$$\forall\, x, y \in A, \qquad \mathscr{C}(x) = \mathscr{C}(y) \iff f(x) = f(y).$$

49.2 L'ensemble quotient A/I est muni d'une structure d'anneau commutatif définie par

$$\begin{aligned} \forall\, x, y \in A, \quad \mathscr{C}(x) \oplus \mathscr{C}(y) &= \mathscr{C}(x + y) \\ \mathscr{C}(x) \otimes \mathscr{C}(y) &= \mathscr{C}(x \star y) \end{aligned}$$

et l'application $\mathscr{C}$ est alors un morphisme d'anneaux surjectif de $(A, +, \star)$ dans $(A/I, \oplus, \otimes)$.
49.3 Il existe un, et un seul, morphisme d'anneaux

$$\varphi : A/I \to B$$

tel que

$$\forall\, x \in A, \quad f(x) = \varphi\big(\mathscr{C}(x)\big).$$

Ce morphisme φ est injectif et, si le morphisme f est surjectif, alors φ est un isomorphisme de A/I sur B.

III

Algèbres et polynômes

50. Soit $\mathbb{K}$, un corps.
50.1 ✍ *Une* **algèbre associative unitaire sur** $\mathbb{K}$ *est un ensemble A muni d'une structure d'espace vectoriel sur $\mathbb{K}$ pour $(+, \cdot)$ et d'une structure d'anneau pour $(+, *)$ telles que*

$$\forall\, (\lambda, x, y) \in \mathbb{K} \times A^2, \quad (\lambda \cdot x) * y = \lambda \cdot (x * y) = x * (\lambda \cdot y).$$

50.2 Dans une algèbre associative unitaire A, si

$$a = \sum_{k=0}^{m} \alpha_k \cdot x_k \quad \text{et} \quad b = \sum_{\ell=0}^{n} \beta_\ell \cdot y_\ell,$$

alors

$$a * b = \sum_{k=0}^{m} \sum_{\ell=0}^{n} (\alpha_k \beta_\ell) \cdot (x_k * y_\ell).$$

50.3 ✍ *La* **dimension** *d'une algèbre $(A, +, *, \cdot)$ est la dimension (finie ou non) de l'espace vectoriel $(A, +, \cdot)$.*
50.4 ✍ *L'***élément unité** *d'une algèbre est l'élément neutre pour la multiplication interne.*
50.5 ✍ *Les* **éléments inversibles** *d'une algèbre sont ceux qui ont un symétrique* dans cette algèbre *pour la multiplication interne.*
50.6 L'ensemble des éléments inversibles d'une algèbre est muni d'une structure de groupe pour $*$.

III.1 Sous-algèbres

51. Sous-algèbres
51.1 ✍ *Une* **sous-algèbre** *de $(A, +, *, \cdot)$ est une partie de A munie d'une structure d'algèbre associative unitaire pour les lois $+$, $*$ et $\cdot$.*
51.2 Les sous-algèbres d'une algèbre sur le corps $\mathbb{K}$ sont aussi des algèbres sur le corps $\mathbb{K}$.

52. Méthodes
52.1 $(A, +, *, \cdot)$ est une algèbre associative unitaire si, et seulement si, $(A, +, \cdot)$ est un espace vectoriel et si $*$ est une loi de composition interne, associative, admettant un élément neutre et bilinéaire de $A \times A$ dans A.
52.2 ⇝ *Une partie B de l'algèbre $(A, +, *, \cdot)$ est une sous-algèbre si, et seulement si, B est un sous-espace vectoriel de $(A, +, \cdot)$ qui contient l'élément unité et stable par $*$.*

Exemples d'algèbres et de sous-algèbres

53.1 Le corps $\mathbb{K}$ est une algèbre sur $\mathbb{K}$ où la multiplication interne et la multiplication externe coïncident.
53.2 L'ensemble $\mathbb{K}[X]$ des polynômes à coefficients dans $\mathbb{K}$ est une algèbre sur $\mathbb{K}$.
53.3 L'ensemble $\mathbb{K}[X^2]$ des polynômes pairs est une sous-algèbre de $\mathbb{K}[X]$.
53.4 L'ensemble $\mathfrak{M}_n(\mathbb{K})$ des matrices carrées est une algèbre.
53.5 Les ensembles $D_n(\mathbb{K})$ des matrices diagonales ; $U_n(\mathbb{K})$ des matrices triangulaires supérieures et $L_n(\mathbb{K})$ des matrices triangulaires inférieures sont des sous-algèbres de $\mathfrak{M}_n(\mathbb{K})$.
53.6 L'ensemble $\mathrm{L}(E)$ des endomorphismes de E est une algèbre, qui a $\circ$ pour multiplication interne.
53.7 L'ensemble $\mathscr{A}(\Omega, A)$ des applications d'un ensemble Ω dans une algèbre $(A, +, *, \cdot)$ est une algèbre dont la multiplication interne $\otimes$ est définie par

$$\forall\, f, g, \quad (f \otimes g) = \big[x \mapsto f(x) * g(x)\big].$$

53.8 Lorsque $\Omega \subset \mathbb{K}$, l'ensemble des applications polynomiales de Ω dans $\mathbb{K}$ est une sous-algèbre de $\mathscr{A}(\Omega, \mathbb{K})$.
54. Soit $(A, +, *, \cdot)$, une algèbre. Le ***commutant*** C_a d'un élément $a \in A$, défini par

$$C_a = \{b \in A\ :\ a * b = b * a\},$$

est une sous-algèbre de A (pas nécessairement commutative).

55. Morphismes d'algèbres

55.1 ✍ *Une application φ d'une algèbre $(A,+,*,\cdot)$ dans une algèbre $(B,+,\otimes,\cdot)$ est un* **morphisme d'algèbres** *lorsque φ est à la fois une application linéaire et un morphisme d'anneaux.*

$$\forall\,(\lambda,x,y)\in\mathbb{K}\times A^2,\quad f(\lambda x+y)=\lambda f(x)+f(y),$$
$$\forall\,(x,y)\in A^2,\quad f(x*y)=f(x)\otimes f(y),$$
$$f(1_A)=1_B.$$

55.2 En particulier, un morphisme d'algèbres possède toutes les propriétés d'un morphisme d'anneaux. →**[29]**

55.3 ▷ *Si $f : A\to B$ est un morphisme d'algèbres bijectif, alors sa bijection réciproque est un morphisme d'algèbres.*

55.4 ▷ *L'image d'un morphisme d'algèbres $f : A\to B$ est une sous-algèbre de B.*

55.5 ▷ *Le noyau d'un morphisme d'algèbres $f : \mathscr{A}\to B$ est à la fois un sous-espace vectoriel et un idéal de A.*

III.2 Action des polynômes sur une algèbre

56. Les règles de calcul de la structure d'***algèbre*** ont pour but de former des expressions polynomiales.

56.1 ✍ *Pour tout polynôme*

$$P=\alpha_0+\alpha_1X+\cdots+\alpha_dX^d\in\mathbb{K}[X]$$

*et tout élément a d'une algèbre A sur le corps $\mathbb{K}$, l'***évaluation en** a **du polynôme** *P est l'élément de l'algèbre A défini par*

$$P(a)=\alpha_0\cdot 1_A+\alpha_1\cdot a+\cdots+\alpha_d\cdot a^d.$$

56.2 On obtient $P(a)$ par ***substitution*** de $a\in A$ à l'indéterminée X. Il serait absurde de prendre $X=a$ dans l'expression de P : cela reviendrait en effet à *déterminer* le type de X.

56.3 Soit a, un élément de l'algèbre $(A,+,*,\cdot)$.

1. $$(1)(a)=1_A$$
2. Quels que soient P, Q dans $\mathbb{K}[X]$ et $\lambda\in\mathbb{K}$,
$$(\lambda P+Q)(a)=\lambda P(a)+Q(a).$$
3. Quels que soient P, Q dans $\mathbb{K}[X]$,
$$(PQ)(a)=P(a)*Q(a)$$
4. Si $P_1=QP_0+R$, alors
$$P_1(a)=Q(a)*P_0(a)+R(a).$$

56.4 ➙ **Morphisme d'évaluation**
Pour tout $a\in A$, l'application $\mathcal{E}_a : \mathbb{K}[X]\to A$ définie par

$$\forall\,P\in\mathbb{K}[X],\quad \mathcal{E}_a(P)=P(a)$$

est un morphisme d'algèbres.

56.5 Si $f : A\to B$ est un morphisme d'algèbres, alors

$$\forall\,P\in\mathbb{K}[X],\ \forall\,a\in A,\quad P\big(f(a)\big)=f\big(P(a)\big).$$

56.6 ➙ *Soit $a\in A$. Si $b\in A$ est inversible, alors*

$$P(b^{-1}*a*b)=b^{-1}*P(a)*b$$

pour tout polynôme $P\in\mathbb{K}[X]$.

57. Sous-algèbre engendrée par un élément

57.1 ✍ *La* **sous-algèbre des polynômes en** *$a\in A$ est l'image du morphisme $\mathcal{E}_a$. Elle est notée $\mathbb{K}[a]$.*

$$\mathbb{K}[a]=\big\{P(a),\ P\in\mathbb{K}[X]\big\}$$

57.2 **Minimalité de** $\mathbb{K}[a]$
Si une sous-algèbre B de A contient l'élément a, alors $\mathbb{K}[a]\subset B$.

57.3 ➙ *La sous-algèbre $\mathbb{K}[a]$ est commutative et*

$$\forall\,P\in\mathbb{K}[X],\quad P(a)*a=a*P(a).$$

58. Idéal annulateur

58.1 ✍ *Les* **polynômes annulateurs de** *$a\in A$ sont les polynômes P tels que $P(a)=0_A$.*

58.2 Un élément $a\in A$ est nilpotent si, et seulement si, il existe $d\in\mathbb{N}$ tel que X^d soit un polynôme annulateur de a.

58.3 ➙ *à tout polynôme annulateur* non nul *de a :*

$$\alpha_0+\alpha_1X+\cdots+\alpha_dX^d$$

correspond une relation de liaison non triviale *dans l'algèbre A :*

$$\alpha_0\cdot 1_A+\alpha_1\cdot a+\cdots+\alpha_d\cdot a^d=0_A.$$

58.4 ✍ *L'ensemble des polynômes annulateurs de $a\in A$ est le noyau du morphisme d'algèbres*

$$\mathcal{E}_a=[P\mapsto P(a)] : \mathbb{K}[X]\to A.$$

On l'appelle **idéal annulateur** *de a.*

58.5 ✍ *Si l'idéal annulateur de a n'est pas réduit à $\{0\}$, alors l'unique polynôme unitaire qui engendre cet idéal est appelé* **polynôme minimal** *de a.* →**[47.3]**

58.6 Si $\varphi : A\to B$ est un isomorphisme d'algèbres, alors $a\in A$ et $\varphi(a)\in B$ ont même polynôme minimal (s'ils en ont un).

58.7 ➙ *Soit A, une algèbre de dimension finie. Tout élément de a admet un polynôme minimal et le degré du polynôme minimal est inférieur à la dimension de A.*

58.8 Toute matrice de $\mathfrak{M}_n(\mathbb{K})$ admet un polynôme minimal.

58.9 Si E est un espace vectoriel de dimension finie, alors tout endomorphisme de E admet un polynôme minimal.

Entraînement

59. Questions pour réfléchir

1. Le sous-espace $\mathbb{K}_n[X]$ est-il une sous-algèbre de $\mathbb{K}[X]$?

2.a L'ensemble $\mathrm{GL}_n(\mathbb{K})$ des matrices inversibles est-il une sous-algèbre de $\mathfrak{M}_n(\mathbb{K})$?

2.b Et l'ensemble $\mathcal{O}_n(\mathbb{R})$ des matrices orthogonales ?

2.c Et l'ensemble $\mathcal{S}_n(\mathbb{R})$ des matrices symétriques ?

2.d Et l'ensemble $U_n^0(\mathbb{K})$ des matrices triangulaires supérieures strictes (dont les coefficients diagonaux sont tous nuls) ?

2.e Et l'ensemble des matrices triangulaires ?

3. Condition pour que l'algèbre $\mathscr{A}(\Omega,E)$ soit une algèbre commutative ?

4. *Suite de* **[54]** – Comparer la sous-algèbre $\mathbb{K}[a]$ et le commutant de a pour $A=\mathfrak{M}_n(\mathbb{K})$ et $a=I_n$.

5. Le noyau d'un morphisme d'algèbres $f : A\to B$ est-il une sous-algèbre de A ?

6. Quels sont les polynômes annulateurs d'un élément nilpotent ?

7. L'élément a d'une algèbre admet un polynôme annulateur non nul si, et seulement si, la famille $(a^k)_{k\in\mathbb{N}}$ est liée.

8. Si $f\in\mathrm{L}(E)$ et $\dim E\geqslant 2$, l'application $[P\mapsto P(f)]$ n'est pas surjective.

60. Soient A et B, deux algèbres. L'ensemble $\mathrm{Hom}(A,B)$ des morphismes d'algèbres de A dans B est une sous-algèbre de l'algèbre $\mathscr{A}(A,B)$ des applications de A dans B.

61. Polynôme minimal d'un endomorphisme

Soit $u\in\mathrm{L}(E)$, un endomorphisme admettant un polynôme minimal μ.

1. Pour tout $x\in E$, l'ensemble
$$\mathcal{N}_x=\big\{P\in\mathbb{K}[X]\ :\ P(u)(x)=0_E\big\}$$
est un idéal de $\mathbb{K}[X]$, engendré par un diviseur de μ.

2. Si μ est scindé à racines simples, alors il existe un vecteur $x\in E$ tel que l'idéal $\mathcal{N}_x$ soit engendré par μ.

62. Morphisme d'évaluation [56]

62.1 Sous-algèbre des applications polynomiales

On considère $A = \mathscr{A}(\Omega, \mathbb{K})$ avec $\Omega \subset \mathbb{K}$.

1. La sous-algèbre $\mathscr{A}_0(\Omega, \mathbb{K})$ des applications polynomiales de Ω dans $\mathbb{K}$ est l'image de $\mathcal{E}_a$ avec $a = [x \mapsto x]$.
2. Le morphisme $\mathcal{E}_a$ est injectif si, et seulement si, Ω est une partie infinie de $\mathbb{K}$.

62.2 Nombres algébriques, nombres transcendants

On suppose que $\mathbb{K} = \mathbb{Q}$ et $A = \mathbb{C}$. Le nombre a est dit ***transcendant*** lorsque $\mathcal{E}_a$ est injective et ***algébrique*** dans le cas contraire.

1. La famille $(x_1, \dots, x_N) \in \mathbb{C}^N$ est liée si, et seulement si, il existe une famille $(m_1, \dots, m_N)$ d'entiers relatifs non tous nuls tels que
$$m_1 x_1 + \cdots + m_N x_N = 0.$$
2. Un nombre a est algébrique si, et seulement si, il existe un polynôme $P \in \mathbb{Z}[X]$, non nul, tel que $P(a) = 0$.
3. On *admet* que π est transcendant. Quelle est la dimension de $\mathbb{C}$ en tant qu'espace vectoriel sur $\mathbb{Q}$?
4. Soit $\mathfrak{P}$, l'ensemble des nombres premiers. La famille $(\ell \mathrm{n}\, p)_{p \in \mathfrak{P}}$ est une famille libre de $\mathbb{C}$. Comparer avec [3].
5. Existe-t-il $a \in \mathbb{C}$ tel que l'application $\mathcal{E}_a$ soit surjective ?
6. Soit $a \in \mathbb{C}$, un nombre algébrique. Le ***polynôme minimal*** de a est l'unique générateur unitaire P_0 de l'idéal annulateur $\operatorname{Ker} \mathcal{E}_a \subset \mathbb{Q}[X]$.

6.a En tant qu'élément de $\mathbb{Q}[X]$, le polynôme P_0 est irréductible.

6.b Si $a \neq 0$, alors le terme constant de P_0 n'est pas nul et il existe un polynôme $P_1 \in \mathbb{Q}[X]$ tel que $a^{-1} = P_1(a)$.

6.c L'algèbre $\mathbb{Q}[a]$ est un sous-corps de $\mathbb{C}$. En tant que $\mathbb{Q}$-espace vectoriel, elle admet
$$(1, a, \dots, a^{d-1})$$
pour base, où $d = \deg P_0$.

63.

1. L'application $[u \mapsto \mathfrak{Mat}_{\mathscr{B}}(u)]$ est un isomorphisme d'algèbres de $\mathrm{L}(E)$ sur $\mathfrak{M}_n(\mathbb{K})$, pour toute base $\mathscr{B}$ de E.
2. L'application $[M \mapsto Q^{-1}MQ]$ est un automorphisme d'algèbre de $\mathfrak{M}_n(\mathbb{K})$ pour toute matrice $Q \in \mathrm{GL}_n(\mathbb{K})$.

2.a L'application $[M \mapsto M^\top]$ est-elle un isomorphisme d'algèbre de $\mathfrak{M}_n(\mathbb{K})$ sur $\mathfrak{M}_n(\mathbb{K})$?

64. Inversibilité d'un polynôme en u

Soit $v \in \mathbb{K}[u]$.

1. Comparer $\mathbb{K}[v]$ et $\mathbb{K}[u]$.
2. On suppose que la dimension de $\mathbb{K}[u]$ est finie. Si v est inversible dans A, alors $v^{-1} \in \mathbb{K}[u]$.

65. Les matrices suivantes ont un polynôme minimal de degré 2.

$$\begin{pmatrix} 3 & 4 & -4 \\ -4 & -5 & 4 \\ -2 & -2 & 1 \end{pmatrix} \qquad \begin{pmatrix} -4 & -6 & 6 \\ 6 & 8 & -6 \\ 3 & 3 & -1 \end{pmatrix}$$
$$\begin{pmatrix} -2 & 0 & 0 \\ -4 & 6 & -6 \\ -6 & 12 & -11 \end{pmatrix} \qquad \begin{pmatrix} 5 & 4 & -4 \\ -4 & -3 & 4 \\ -2 & -2 & 3 \end{pmatrix}$$

66. Les matrices suivantes ont un polynôme minimal de degré 3.

$$\begin{pmatrix} 0 & -2 & 2 \\ -7 & -11 & 10 \\ -8 & -14 & 13 \end{pmatrix} \qquad \begin{pmatrix} -7 & -8 & 8 \\ 2 & -1 & 0 \\ -2 & -6 & 5 \end{pmatrix}$$
$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & 3 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 & 0 \\ 7 & 10 & -8 \\ 8 & 12 & -9 \end{pmatrix}$$

Questions, exercices & problèmes

Perfectionnement

67. Exemples et contre-exemples

1. Les matrices
$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$
sont des éléments nilpotents de l'anneau $\mathfrak{M}_2(\mathbb{K})$, mais les produits AB et BA ne sont pas nilpotents.
2. Exemples de groupes cycliques ; de groupes non cycliques.
3. Exemples d'algèbres commutatives ? non commutatives ?
4. Exemples d'algèbres de dimension finie ? de dimension infinie ?
5. Existe-t-il une sous-algèbre de $\mathbb{K}[X]$ qui ne soit pas de la forme $\mathbb{K}[X^n]$?

68. Méthodes

1. Comment déterminer l'ordre d'un élément ?
2. Comment vérifier si un groupe est cyclique ?
3. Construire un algorithme qui calcule la table **[72]**.
4. Comment calculer le polynôme minimal **[58.5]** d'une matrice $A \in \mathfrak{M}_3(\mathbb{K})$?

69. Questions pour réfléchir

1. Quels algorithmes reposent-ils sur les factorisations du groupe symétrique **[3.4]** ? du groupe linéaire **[3.5]** ?
2. Un groupe d'ordre n contient-il un élément d'ordre n ?
3. Pourquoi le groupe $\mathfrak{S}_3$ n'est-il pas cyclique ?
4. Un diviseur de zéro est-il toujours nilpotent ?
5. Tout sous-anneau d'un corps est intègre. Réciproquement, tout anneau intègre est en quelque sorte contenu dans un corps (***corps des fractions***).
6. *Suite de* **[64]** – Étudier le cas où la dimension de $\mathbb{K}[u]$ est infinie.

Approfondissement

70. Quaternions

On considère les quatre matrices complexes $I = I_2$,
$$J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad L = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$$
et on note $\mathbb{H}$, l'espace vectoriel *réel* engendré par ces matrices.
$$\mathbb{H} = \left\{ aI + bJ + cK + dL,\ (a, b, c, d) \in \mathbb{R}^4 \right\} \subset \mathfrak{M}_2(\mathbb{C})$$
L'ensemble $\mathbb{H}$ des ***quaternions*** est une algèbre de dimension 4 sur $\mathbb{R}$ ainsi qu'un corps *non* commutatif dont un sous-corps est isomorphe à $\mathbb{C}$.

71. Exemples de parties génératrices

71.1 Le sous-groupe alterné $\mathfrak{A}_n$, constitué des permutations $\sigma \in \mathfrak{S}_n$ dont la signature est égale à 1, est engendré par les cycles de longueur 3.

71.2 Algorithme du pivot

1. Le sous-groupe $\mathrm{SL}_n(\mathbb{R})$ des matrices dont le déterminant est égal à 1 est engendré par les matrices de transvection.
2. L'ensemble $\mathrm{SL}_2(\mathbb{Z})$ des matrices de $\mathfrak{M}_2(\mathbb{Z})$ dont le déterminant est égal à 1 est un groupe pour $\times$. Il est engendré par les matrices
$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

71.3 Le groupe produit additif $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ est engendré par $(\mathscr{C}_2(1), \mathscr{C}_3(1))$.

72. Groupe diédral d'ordre 8
Le ***groupe diédral*** est le sous-groupe G de $\mathrm{GL}_2(\mathbb{R})$ engendré par les deux matrices

$$S = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

1. L'ensemble G est un sous-groupe de $O_2(\mathbb{R})$.
2. Comme $TS = ST^3$, alors

$$G = \{I_2, S, T, ST, T^2, ST^2, T^3, ST^3\}$$

et la table de multiplication de G est

	I_2	S	T	ST	T^2	ST^2	T^3	ST^3
$I_2\times$	I_2	S	T	ST	T^2	ST^2	T^3	ST^3
$S\times$	S	I_2	ST	T	ST^2	T^2	ST^3	T^3
$T\times$	T	ST^3	T^2	S	T^3	ST	I_2	ST^2
$ST\times$	ST	T^3	ST^2	I_2	ST^3	T	S	T^2
$T^2\times$	T^2	ST^2	T^3	ST^3	I_2	S	T	ST
$ST^2\times$	ST^2	T^2	ST^3	T^3	S	I_2	ST	T
$T^3\times$	T^3	ST	I_2	ST^2	T	ST^3	T^2	S
$ST^3\times$	ST^3	T	S	T^2	ST	T^3	ST^2	I_2

3. Le groupe $(G, \times)$ n'est pas isomorphe à $(\mathbb{U}_8, \times)$, ni à $(\mathbb{U}_2 \times \mathbb{U}_4, \times)$, ni à $(\mathbb{U}_2 \times \mathbb{U}_2 \times \mathbb{U}_2, \times)$.
4. L'ensemble des automorphismes de $\mathbb{R}^2$ qui laissent le carré unité globalement invariant est isomorphe au groupe G.

à chaque polygone régulier d'ordre $2n$ (carré, hexagone, octogone...) correspond un sous-groupe de $\mathrm{SO}_2(\mathbb{R})$ qui est l'ensemble des automorphismes de $\mathbb{R}^2$ qui laissent ce polygone globalement invariant.

Pour aller plus loin

73. Soient A, un anneau intègre et I, un idéal de A. L'ensemble

$$J = \{x \in A \,:\, \exists\, n \in \mathbb{N},\ x^n \in I\}$$

est un idéal de A.

74. Démonstration du théorème de Lagrange [14.2]
On pose H, un sous-groupe de G et, pour tout $x \in G$,

$$xH = \{x \star y,\ y \in H\}.$$

1. Quel que soit $x \in G$, l'ensemble xH est l'image de H par la translation $[y \mapsto x \star y]$, donc le cardinal de xH est égal au cardinal de H et

$$xH = H \iff x \in H.$$

2. La relation $\mathscr{R}$ définie par

$$x \mathscr{R} y \iff xH = yH$$

est une relation d'équivalence sur G.
3. Si $x_1H \cap x_2H \neq \varnothing$, alors $x_1H = x_2H$.
4. Il existe $x_1, \ldots, x_q$ dans G tels que

$$G = \bigsqcup_{1 \leqslant k \leqslant q} x_k H$$

donc le cardinal de H divise l'ordre de G.

75. Applications polynomiales
Nous parlerons ici de *polynômes* alors qu'il s'agit en fait de *fonctions polynomiales*.

75.1 ✍ *Un* **monôme en** d **variables** *est une application de* $\mathbb{K}^d$ *dans* $\mathbb{K}$ *de la forme*

$$\left[x = (x_1, \ldots, x_d) \mapsto x_1^{k_1} \cdots x_d^{k_d}\right]$$

où $(k_1, \ldots, k_d) \in \mathbb{N}^d$.

75.2 ✍ *L'espace des* **polynômes en** d **variables**, *noté* $\mathbb{K}[x_1, \ldots, x_d]$, *est le sous-espace de* $\mathscr{A}(\mathbb{K}^d, \mathbb{K})$ *engendré par les monômes.*
75.3 ➙ *L'ensemble* $\mathbb{K}[x_1, \ldots, x_d]$ *des polynômes en d variables est une algèbre associative unitaire.*
75.4 Notation courte
Pour tout vecteur $x = (x_1, \ldots, x_d) \in \mathbb{K}^d$ et tout ***multi-indice***

$$k = (k_1, \ldots, k_d) \in \mathbb{N}^d,$$

le produit

$$x_1^{k_1} \cdots x_d^{k_d} \in \mathbb{K}$$

sera noté simplement x^k.
Le produit x^k est nul si, et seulement si, l'une des coordonnées $x_1, \ldots, x_d$ est nulle.
75.5 ➙ *Étant donnés deux multi-indices k et* ℓ *dans* $\mathbb{N}^d$,

$$\forall\, x \in \mathbb{K}^d, \quad x^{k+\ell} = x^k x^\ell.$$

75.6 Base canonique de $\mathbb{K}[x_1, \ldots, x_d]$
1. Si la fonction polynomiale

$$\left[x \mapsto \sum_{k \in \mathbb{N}} \alpha_k x^k\right]$$

de $\mathbb{K}$ dans $\mathbb{K}$ est identiquement nulle sur $\mathbb{K}$, alors tous les coefficients α_k sont nuls.
2. Si $d \geqslant 2$, un polynôme de $\mathbb{K}[x_1, \ldots, x_d]$ peut être considéré comme une fonction polynomiale en une variable x_d à coefficients dans $\mathbb{K}[x_1, \ldots, x_{d-1}]$.
3. Pour tout $d \geqslant 1$ et tout polynôme $P \in \mathbb{K}[x_1, \ldots, x_d]$, il existe une, et une seule, famille presque nulle $(\alpha_k)_{k \in \mathbb{N}^d}$ telle que

$$\forall\, x \in \mathbb{K}^d, \quad P(x) = \sum_{k \in \mathbb{N}^d} \alpha_k x^k.$$

4. On suppose que l'application polynomiale définie par

$$\forall\, x \in \mathbb{K}^d, \quad P(x) = \sum_{k \in \mathbb{N}^d} \alpha_k x^k$$

est identiquement nulle sur une partie Ω de $\mathbb{K}^d$.

4.a Si $\Omega = \mathbb{K}^d$, alors tous les coefficients α_k sont nuls.

4.b Il existe une partie infinie $\Omega_0 \subset \mathbb{R}^2$ telle que l'application polynomiale définie sur $\mathbb{R}^2$ par

$$P_0(x, y) = x^2 + y^2 - 1$$

soit identiquement nulle sur Ω alors que ses coefficients ne sont pas tous nuls.

4.c Condition suffisante sur $\Omega \subset \mathbb{K}^d$ pour que les coefficients de P soient tous nuls ?

75.7 ✍ **Degré d'un polynôme en** d **variables**
Si $k = (k_1, \ldots, k_d) \in \mathbb{N}^d$, *le* **degré** *du monôme* $[x \mapsto x^k]$ *est*

$$|k| = \sum_{i=1}^{d} k_i.$$

75.8 à tout polynôme $[x \mapsto \sum_{k \in \mathbb{N}^d} \alpha_k x^k]$ de $\mathbb{K}[x_1, \ldots, x_d]$, on associe les ensembles

$$K = \{k \in \mathbb{N}^d \,:\, \alpha_k \neq 0\} \subset \mathbb{N}^d \quad \text{et} \quad |K| = \{|k|,\ k \in K\} \subset \mathbb{N}.$$

5. Les ensembles K et $|K|$ sont finis.
6. Un polynôme est un monôme si, et seulement si, K est un singleton.

75.9 ✍ *Un polynôme est* **homogène** *lorsque l'ensemble* $|K|$ *est un singleton.*
75.10 ✍ *Le* **degré d'un polynôme** *est* $\max(|K|)$. *Sa* **valuation** *est* $\min(|K|)$.

7. Que dire du degré de la somme de deux polynômes ?
8. Écrire la formule donnant le produit de deux applications polynomiales. Que dire du degré du produit de deux polynômes ?